Aussagenlogik

- Syntax
- Semantik
- Formeln, Modelle, Tautologien und Anwendungen
- Folgerungen, Wissen
- Syntaktisch besondere Formeln und Formelgraphen, wichtige Algorithmen
- **Axiomatiken, Kalküle**

Jeder korrekte axiomatisch-deduktive Kalkül

… verwendet:

- Junktorenbasis ***Ju***
  … definiert „repräsentative" Formelmenge **Form(*Ju*)**:
  - sie produzieren alle Wahrheitswerteverläufe, und
  - zu jeder AL-Formel gibt es eine äquivalente *Ju*-Formel.

- Menge ***Ax*** von **Axiomen**,
  ausgewählte AL-Tautologien über *Ju*

- Menge ***Reg*** von **Inferenz-** oder **Ableitungsregeln**,
  ausgewählte AL-Folgerungen aus endlichen Formelmengen
  $\{\varphi_1, ..., \varphi_n\} \vDash \psi$,
  allesamt *Ju*-Formeln.

Ableitungsschritt

Anwendung eines Axioms ψ bedeutet:

- Wahl einer Substitution z = $A_1, ..., A_k / \pi_1, ..., \pi_k$ und
- Aufnahme von $\psi_{[z]}$ in die Menge der abgeleiteten Formeln.
- Man schreibt auch $|-_{\psi}\ \psi_{[z]}$.

Anwendung einer Regel R: $\{\varphi_1, ..., \varphi_n\} \models \psi$ bedeutet:

- Wahl einer Substitution z = $A_1, ..., A_k / \pi_1, ..., \pi_k$, derart, dass $\varphi_{1[z]}, ..., \varphi_{n[z]}$ bereits abgeleitet sind, und
- Aufnahme von $\psi_{[z]}$ in die Menge der abgeleiteten Formeln.
- Man schreibt auch $\varphi_{1[z]}, ..., \varphi_{n[z]} \vdash_R \psi_{[z]}$.

Anwendungsbeispiel: Ist R : $A \wedge B \models A \vee B$ und z = $A, B / C, D \rightarrow E$ und die Formel $C \wedge (D \rightarrow E)$ bereits abgeleitet, so erzeugt ein Ableitungsschritt mit R die Formel $C \vee (D \rightarrow E)$: $C \wedge (D \rightarrow E) \vdash C \vee (D \rightarrow E)$

Regeln

Axiome sind praktisch spezielle Regeln $\emptyset \models \psi$ mit leerer Menge von Prämissen.
Wir reden daher jetzt oft einfach nur noch von **Regeln**.

Die wichtigste Inferenzregel ist der Modus Ponens
$\boxed{\mathrm{MP} : A,\ \ A \to B\ \models\ B}$.

Vollständigkeit

Den Kalkül nennt man **vollständig**, wenn es möglich ist,
durch wiederholte Anwendung der Axiome und Regeln

- **alle Tautologien** über *Ju* und
- bei Vorgabe einer Wissensbasis $M \subseteq \mathrm{Form}(Ju)$
  alle Folgerungen aus M (über *Ju*) abzuleiten.

Ableitbare Formeln

Aus Formelmenge ableitbare Formeln:

Induktiv

φ ist mittels eines Kalküls (*Ju*,*Reg*) **aus** $\boldsymbol{M}\subseteq$Form(Ju) **ableitbar**, wenn:

- $\varphi \in M$ oder
- es existiert Menge M' aus M ableitbarer Formeln und Regel $R\in Reg$ derart, dass φ mittels R (und Substitution) in einem Schritt aus M' ableitbar ist, $M' \vdash_R \varphi$.

Iterativ

Menge der mittels eines Kalküls (*Ju*,*Reg*) **aus** $\boldsymbol{M}\subseteq$Form(Ju) **ableitbar**en Formeln:

- $\mathrm{Abl}^0_{Reg}(M) \coloneqq M$
- $\mathrm{Abl}^{n+1}_{Reg}(M) \coloneqq \mathrm{Abl}^n_{Reg}(M) \cup \bigcup_{R\in Reg} \{\varphi \in Form \mid \mathrm{Abl}^n_{Reg}(M) \vdash_R \varphi\}$
- $\mathrm{Abl}_{Reg}(M) \coloneqq \bigcup_{n=1}^{\infty} \mathrm{Abl}^n_{Reg}(M)$.

Ableitung, Beweis

Ableitung/Beweis einer Formel φ (aus M mit Reg) :=

endliche Folge $\varphi_1, ..., \varphi_n$ mit $\varphi = \varphi_n$ und derart, dass jedes φ_k in M oder aus davorstehenden Formeln unmittelbar ableitbar ist: $\varphi_k \in \mathrm{Abl}^1_{Reg}(\{\varphi_1, ..., \varphi_{k-1}\})$.

Kalkülbeispiele (1)

	Hilbert-Ackermann	
Junktorenbasis	$\neg, \vee$	
Axiome	$\neg(A \vee A) \vee A$	$\neg(A \vee B) \vee (B \vee A)$
	$\neg A \vee (A \vee B)$	$\neg(\neg A \vee B) \vee (\neg(C \vee A) \vee (C \vee B))$
Inferenzregeln	Modifizierter Modus Ponens MMP $= \dfrac{A, \neg A \vee B}{B}$	

	Mendelson
Junktorenbasis	$\neg, \rightarrow$
Axiome	$A \rightarrow (B \rightarrow A)$
	$(A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C))$
	$(\neg B \rightarrow \neg A) \rightarrow ((\neg B \rightarrow A) \rightarrow B)$
Inferenzregeln	Modus Ponens

Beide sind **ableitungs-** (und beweis-) **korrekt** und **vollständig**.

Kalkülbeispiele (2)

Mit Geschick **reicht ein einziges** (recht langes) **Axiom.**

Es gab schon „sportliche Wettläufe" um das
jeweils **kürzeste** einzige Axiom in einer Junktorenbasis.

Andere Axiomensysteme spendieren **mehr Axiome**:

Hilbert-Bernays, Kleene, de Swart, ...

Beweisbeispiele (1)

Beweis = Ableitung aus den Axiomen!

$\boxed{A \to A \text{ im Mendelson-Kalkül}}$

1. $(A \to (B \to C)) \to ((A \to B) \to (A \to C))$ — Axiom
2. $(A \to ((A \to A) \to A)) \to ((A \to (A \to A)) \to (A \to A))$ — 1, $[B, C \,/\, A \to A, A]$
3. $A \to (B \to A)$ — Axiom
4. $A \to ((A \to A) \to A)$ — 3, $[B \,/\, A \to A]$
5. $((A \to (A \to A)) \to (A \to A))$ — 2, 4, MP
6. $A \to (A \to A)$ — 3, $[B \,/\, A]$
7. $A \to A$ — 5, 6, MP

Beweisbeispiele (2)

$A \to A$ (d.h. $\neg A \lor A$) im Hilbert-Ackermann-Kalkül

1. $\neg(\neg A \lor B) \lor (\neg(C \lor A) \lor (C \lor B))$	Axiom
2. $\neg(\neg A \lor B) \lor (\neg(\neg C \lor A) \lor (\neg C \lor B))$	1, $C / \neg C$
3. $\neg A \lor (A \lor B)$	Axiom
4. $\neg A \lor (A \lor A)$	3, B / A
5. $\neg(\neg(A \lor A) \lor A) \lor (\neg(\neg A \lor (A \lor A)) \lor (\neg A \lor A))$	2, $A, B, C / A \lor A, A, A$
6. $\neg(\neg A \lor (A \lor A)) \lor (\neg A \lor A)$	4,5,MMP
7. $\neg A \lor A$	4,6,MMP

Leichter nachzuprüfen als darauf zu kommen!

Ü36

Berechtigte Fragen (1)

Wozu Kalküle und Beweise?
Wir haben doch unsere Wahrheitstafeln und sonstigen Algorithmen! :-)

(1) **Komplexität**

Man beweist lieber $(A \wedge B \wedge C \wedge D \wedge E \wedge F \wedge G) \rightarrow A$ in wenigen Schritten im Kalkül als mittels Wahrheitstafel mit 128 Zeilen und 1792 Feldern.

(2) **Berechenbarkeit**

In der vollen Prädikatenlogik handeln die „Formeln“ von Eigenschaften von potentiell **unendlich vielen verschiedenen Objekten**. Die kann man **nicht** mehr alle in einer **Tabelle** erfassen und durchrechnen.
Da gibt es (beweisbar!) **keinen** sicher terminierenden **Algorithmus** zur Überprüfung der Erfüllbarkeit etc. – wir **sind auf Beweise angewiesen**.

:-(

Berechtigte Fragen (2)

Na gut, dann umgekehrt:
Wozu diese ganzen Wahrheitstafeln und sonstigen Algorithmen? :-(

In vielen praktischen Fragen gelingt es, das Ganze in Aussagenlogik auszudrücken. Und dann kann man zum Glück den Computer die algorithmische Arbeit erledigen lassen. :-)

Natürliches Schließen und unser Werkzeugkasten

In den 1930er Jahren erweiterte Gerhard Gentzen die axiomatischen Kalküle gewissermaßen um das Deduktionstheorem und erhielt so seinen (formalen) **Kalkül des natürlichen Schließens**, der weitgehend das formlose Beweisen in Mathematikbüchern streng formal nachbildet.

Seine Beweise sind nicht reine **Folgen** von Formeln, wie im Vorigen, sondern haben teilweise eine **Blockstruktur**:

Annahme: φ

Hier darf φ benutzt werden.

$\vdots$

ψ

$\varphi \to \psi$

+ die bisher abgeleiteten Formeln,
+ die noch von oben geltenden Annahmen (aus umgebenden Blöcken)

bedingter Beweis

GNS-Beispiel

Ableitung von $(A \to B) \to ((B \to C) \to (A \to C))$

nach unserer GNS-Definition, annotiert,
in einer Baumschreibweise mit Einrückung
(traditionelle Schreibweise anders):

Nr.	Formel	Regel,-Pr.
1	Ann: $A \to B$	AE
2	Ann: $B \to C$	AE
3	Ann: A	AE
4	B	FB,1,3
5	C	FB,2,4
6	$A \to C$	FE,3,5
7	$(B \to C) \to (A \to C)$	FE,2,6
8	$(A \to B) \to ((B \to C) \to (A \to C))$	FE,1,7

GNS-Beispiel, historisch

$\boxed{\text{Ableitung von } (A \to B) \to ((B \to C) \to (A \to C))}$

traditionelle Schreibweise

$$
\begin{prooftree}
\AxiomC{$[A]_1$}
\AxiomC{$[A \to B]_3$}
\RightLabel{FB}
\BinaryInfC{B}
\AxiomC{$[B \to C]_2$}
\RightLabel{FB}
\BinaryInfC{C}
\RightLabel{FE$_1$}
\UnaryInfC{$A \to C$}
\RightLabel{FE$_2$}
\UnaryInfC{$(B \to C) \to (A \to C)$}
\RightLabel{FE$_3$}
\UnaryInfC{$(A \to B) \to ((B \to C) \to (A \to C))$}
\end{prooftree}
$$

Beispiel in „Werkzeugkastenversion“

Zeige $(A \to B) \to ((B \to C) \to (A \to C))$

Zielfor-mulierung → *begin*

1.	$\mid\quad A \to B$	Ann
	$\mid\quad$ Zeige $(B \to C) \to (A \to C)$	
2.	$\mid\quad\mid\quad B \to C$	Ann
	$\mid\quad\mid\quad$ Zeige $(A \to C)$	
3.	$\mid\quad\mid\quad\mid\quad A$	Ann
4.	$\mid\quad\mid\quad\mid\quad B$	MP,1,3
5.	$\mid\quad\mid\quad\mid\quad C$	MP,2,4
6.	$\mid\quad\mid\quad A \to C$	BB
7.	$\mid\quad (B \to C) \to (A \to C)$	BB
8.	$(A \to B) \to ((B \to C) \to (A \to C))$	BB

Ziel erreicht → *end*

Unser Werkzeugkasten (erweitertes GNS) wird noch **weitere Regeln** enthalten, und die damit gebauten Beweise werden sehr „natürlich“ und doch **exakt** sein.

Werkzeugkasten – Beweisaufbau – Zeilentypen

ohne **Ableitungsbegründung:**

1. Zuerst die **Prämissen**
   Ausgangsannahmen, aus denen gefolgert werden soll – sofern vorhanden: keine bei Beweisen von Tautologien: φ Gegeben
2. **Zielformeln** (eine erste unmittelbar nach den Prämissen): **`Zeige`** φ
3. ad hoc **angenommene Formeln**, für IB/BB-Blöcke: φ Annahme

mit **Ableitungsbegründung:**

4. **abgeleitete Formeln**: φ Regel, Prämissennummer(n)
   speziell: Erfüllungszeilen φ Beweistyp (DB/IB/BB)

Alle (außer Zielformeln) sind jeweils durchnummeriert – wegen späterer Verweise als Prämissennummern.

Werkzeugkasten – Beweisaufbau – Blöcke

- Auf die Prämissen folgt der **Haupt-Block**.

5. Ein **Block** beginnt mit einer **Zielzeile** (`Zeige` φ),

   dann kommt (eingerückt) der **Blockkörper**,

   Die **letzte** Formel im eingerückten Blockkörper muss jeweils **abgeleitet** sein.

   am Ende (nicht mehr eingerückt) die Erfüllungszeile φ.

- Es gibt 4 Blockschemata, den 4 Beweismethoden entsprechend, → Tabelle.

- Im Blockkörper stehen **angenommene** Formeln und Erfüllungszeilen nur dort, wo im Blockschema gezeigt (oder entsprechend in Unterblöcken), abgeleitete Formeln und **Unterblöcke** (**Zwischenbeweise**) aber nach Belieben.

Wie wird abgeleitet?

- per **Blockschema/Beweismethode**

oder

- per **Ableitungsregeln/Schlussregeln**
  → Tabelle
  In der Regelanwendung verfügbare Voraussetzungen (Prämissen) sind frühere Formeln aus dem laufenden oder dessen umgebenden Blöcken.

Beweis-Methoden (1)

a) **Direkter Beweis**
Blockbeginn: **`Zeige`** φ.
Sobald im **Blockkörper** φ abgeleitet, …
Blockende: Erfüllungszeile φ **`DB`**.

… dienen der Zerlegung in Teilaufgaben.

b) **Bedingter Beweis**
Blockbeginn: **`Zeige`** $\varphi \rightarrow \psi$**,**
Annahmezeile φ **`Ann`**
Sobald im gleichen Block ψ abgeleitet, …
Blockende: Erfüllungszeile $\varphi \rightarrow \psi$ **`BB`**.

Direkter Beweis:
Zeige φ
| $\vdots$
(| φ) *weglassbar s.u.*
φ DB

Bedingter Beweis:
Zeige $\varphi \rightarrow \psi$
| φ Ann
| $\vdots$
| ψ
$\varphi \rightarrow \psi$ BB

(Zwischen) Beweis-Methoden (2)

c) **Indirekter Beweis 1**
Blockbeginn: `Zeige` φ,
im Blockkörper unmittelbar gefolgt von $\neg\varphi$ **`Ann`**
Sobald im Blockkörper $\bot$ (Widerspruch) abgeleitet, …
Blockende: φ **`IB1`**

d) **Indirekter Beweis 2**
Blockbeginn: Zeige $\neg\varphi$,
im Blockkörper unmittelbar gefolgt von φ **`Ann`**
Sobald im gleichen Block $\bot$ (Widerspruch) abgeleitet, …
Blockende: $\neg\varphi$ **`IB2`**

Indirekter Beweis 1:
Zeige φ
| $\neg\varphi$ Ann
| $\vdots$
| $\bot$
φ IB1

Indirekter Beweis 2:
Zeige $\neg\varphi$
| φ Ann
| $\vdots$
| $\bot$
$\neg\varphi$ IB2

Werkzeugkasten – Schlussregeln (1)

Oder-Einführung	OE $\dfrac{\varphi}{\varphi \vee \psi}, \dfrac{\psi}{\varphi \vee \psi}$	Oder-Benutzung 1	OB_1 $\dfrac{\varphi \vee \psi, \neg\varphi}{\psi}, \dfrac{\varphi \vee \psi, \neg\psi}{\varphi}$
Und-Einführung	UE $\dfrac{\varphi, \psi}{\varphi \wedge \psi}$	Oder-Benutzung 2	OB_2 $\dfrac{\varphi \vee \psi, \varphi \to \rho, \psi \to \rho}{\rho}$
Und-Benutzung	UB $\dfrac{\varphi \wedge \psi}{\varphi}, \dfrac{\varphi \wedge \psi}{\psi}$	Wieder-holung	WDH $\dfrac{\varphi}{\varphi}$
Doppelte Negations-Einführung	DNE $\dfrac{\varphi}{\neg\neg\varphi}$	Doppelte-Negation-Benutzung	DNB $\dfrac{\neg\neg\varphi}{\varphi}$
Gdw-Einführung	GE $\dfrac{\varphi \to \psi, \psi \to \varphi}{\varphi \leftrightarrow \psi}$	Gdw-Benutzung links/ rechts	GB $\dfrac{\varphi \leftrightarrow \psi}{\varphi \to \psi}, \dfrac{\varphi \leftrightarrow \psi}{\psi \to \varphi}$
Widerspr.-Einführung	WE $\dfrac{\varphi, \neg\varphi}{\bot}$	Widerspruch-Benutzung	WB $\dfrac{\bot}{\varphi}$
Folgerungs-Benutzung Modus Ponens	MP $\dfrac{\varphi, \varphi \to \psi}{\psi}$	Folgerungs-Benutzung Modus Tollens	MT $\dfrac{\varphi \to \psi, \neg\psi}{\neg\varphi}$

Werkzeugkasten – Schlussregeln (2)

Nicht-Und-Benutzung	NUB $\dfrac{\neg(\varphi \wedge \psi)}{\varphi \to \neg\psi}, \dfrac{\neg(\varphi \wedge \psi)}{\psi \to \neg\varphi}$	Nicht-Oder-Benutzung	NOB $\dfrac{\neg(\varphi \vee \psi)}{\neg\varphi}, \dfrac{\neg(\varphi \vee \psi)}{\neg\psi}$
Nicht-Folgerungs-Benutzung	NFB $\dfrac{\neg(\varphi \to \psi)}{\varphi \wedge \neg\psi}$	Nicht-Gdw-Benutzung	NGB $\dfrac{\neg(\varphi \leftrightarrow \psi)}{\neg\varphi \leftrightarrow \psi}, \dfrac{\neg(\varphi \leftrightarrow \psi)}{\varphi \leftrightarrow \neg\psi}$

Weitere Regeln sind aus Äquivalenz- und Implikation-Tautologien **herleitbar**.

Modularität: Sinnvoll ist in der **Praxis** auch das Einfügen von *anderswo bewiesenen* Tautologien oder Folgerungen aus *M* (mit einer Quellenangabe an Stelle der **Ableitungsbegründung**).
Autoren von Mathematikbüchern zitieren z.B. oft früher (im gleichen Buch oder anderswo) bewiesene „Sätze“ in Beweisen späterer Sätze, anstatt deren komplette Beweise in den neuen Beweis einzubauen.

Werkzeugkasten – 3 Beweisstrategien

Zeige $\varphi \wedge \psi$		Zeige $\varphi \leftrightarrow \psi$		Zeige $\varphi \vee \psi$	
$\mid$ Zeige φ		$\mid$ Zeige $\varphi \rightarrow \psi$		$\mid \neg(\varphi \vee \psi)$	AE
$\mid \quad \mid \ \vdots$		$\mid \quad \mid \ \vdots$		$\mid \neg\varphi$	NOB
$\mid \quad \varphi$		$\mid \quad \varphi \rightarrow \psi$		$\mid \neg\psi$	NOB
$\mid$ Zeige ψ		$\mid$ Zeige $\psi \rightarrow \varphi$		$\mid \quad \mid \ \vdots$	
$\mid \quad \mid \ \vdots$		$\mid \quad \mid \ \vdots$		$\mid \quad \bot$	
$\mid \quad \psi$		$\mid \quad \psi \rightarrow \varphi$		$\varphi \vee \psi$	IB1
$\varphi \wedge \psi$	UE	$\varphi \leftrightarrow \psi$	GE		

Werkzeugkasten – Nutzen

Satz: Der **Werkeugkasten** für **Aussagenlogik** ist (ableitungs- und beweis-) **korrekt** und **vollständig**.

Der Werkeugkasten **formalisiert** die **manuell** üblichen Beweise und macht sie dadurch maschinell überprüfbar.

Aber er führt (wie manuelle Beweisversuche) **nicht zwingend** zum Beweis einer korrekten Tautologie oder Folgerung.

Er verwendet implizit das **Deduktionstheorem** (siehe bedingter Beweis). Dies erlaubt **kürzere Beweise** als z.B. nur mit Axiomen und Modus Ponens.

Vergleich axiomatischer und Werkzeugkasten-Beweis

Erinnerung:

$\boxed{A \to A \text{ im Mendelson-Kalkül}}$

1.	$(A \to (B \to C)) \to ((A \to B) \to (A \to C))$	Axiom
2.	$(A \to ((A \to A) \to A)) \to ((A \to (A \to A)) \to (A \to A))$	1, $[B, C \,/\, A \to A, A]$
3.	$A \to (B \to A)$	Axiom
4.	$A \to ((A \to A) \to A)$	3, $[B \,/\, A \to A]$
5.	$((A \to (A \to A)) \to (A \to A))$	2, 4, MP
6.	$A \to (A \to A)$	3, $[B \,/\, A]$
7.	$A \to A$	5, 6, MP

Neu:

$\boxed{A \to A \text{ – mit Werkzeugkasten}}$

Zeige $A \to A$

1.	$\mid\; A$	Ann
2.	$\mid\; A$	Wdh, 1
3.	$A \to A$	BB

Ü38

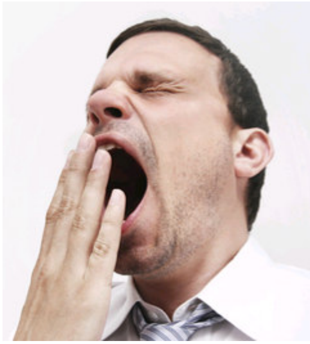
Ü37

Ü39

Exkurs: Interessante mathematische Sätze über AL

Mathematiker

- **Interpolationssätze**
- **Kompaktheitssätze**



Nichtmathematiker

Interpolationssätze der AL

Craigs Interpolationssatz für AL

Wenn für zwei Formeln φ, ψ gilt: $\boxed{\models \varphi \to \psi}$, dann

- kommt entweder eine Aussagevariable *P* sowohl in φ als auch in ψ vor, und dann existiert auch eine Formel π, deren sämtliche Aussagevariablen sowohl in φ als auch in ψ vorkommen, derart dass $\boxed{\models \varphi \to \pi}$ und $\boxed{\models \pi \to \psi}$.
- oder sie haben keine Aussagevariable gemeinsam, und $\boxed{\models \neg\varphi}$ oder $\boxed{\models \psi}$.

Beweis (mit **Konstruktion** für ein π): Wikipedia (englisch) – Craig interpolation

Lyndons Interpolationssatz für AL

E12

- Wenn sich zwei Theorien *S*, *T* widersprechen, d.h. wenn für zwei Theorien *S*, *T* Theo($S \cup T$) unerfüllbar ist, dann existiert eine Formel φ, deren sämtliche Aussagevariablen sowohl in *S* als auch in *T* vorkommen und derart dass $\boxed{S \models \varphi}$ und $\boxed{T \models \neg\varphi}$ ... (+ weitere Eigenschaften von φ)

Kompaktheitssätze der AL

- Eine Formelmenge ***M*** ist **erfüllbar** genau dann, wenn **jede endliche Teilmenge von *M* erfüllbar** ist.

nette Übung in Prädikatenlogik und Mengenlehre

- Aus einer Formelmenge ***M*** **folgt** eine Formel ψ, $M \models \psi$, genau dann, wenn ψ bereits aus **einer endlichen Teilmenge** $N \subseteq M$ folgt: $N \models \psi$.

Ein möglicher Beweisweg der **oberen Aussage** für **abzählbare** *M* verwendet **Königs Lemma**.
Für **beliebige** *M* aber verwendet man das **Lemma von Zorn**:

> In jeder nicht-leeren partiellen Ordnung,
> in der jede Kette nach oben beschränkt ist,
> existiert ein maximales Element.

Das geht aber nur in einer Mengenlehre mit **Auswahlaxiom**.

Das Auswahlaxiom kommt den meisten intuitiv **selbstverständlich** vor, hat aber Konsequenzen, die den meisten (zunächst?) intuitiv **falsch** vorkommen.
→ **Banach-Tarski-Paradoxon**